UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/801,070	03/15/2004	Scott J. Healy	279.718US1	1240

21186 7590 02/06/2006

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH
1600 TCF TOWER
121 SOUTH EIGHT STREET
MINNEAPOLIS, MN 55402

EXAMINER	
PATEL, JOY	

ART UNIT	PAPER NUMBER
3766	

DATE MAILED: 02/06/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/801,070	HEALY ET AL.	
	Examiner	Art Unit	
	Joy P. Patel	3766	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 November 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18,25-30 and 47-59* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18,25-30,47-49,53 and 56-59* is/are rejected.

7)☒ Claim(s) *50-52,54 and 55* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *March 15, 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 3/30/05 8/10/05, 11/28/05
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Objections

1. Claim 52 is objected to because of the following informalities: The step of calculating a third hash value is never mentioned in the specifications. Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1, 6-11, 13-16, 25-30, 47, 53, and 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mazar et al. (US 2004/0122489) in view of Abdulkader (US 2002/0120838).

3. In regard to claims 1 and 10, Mazar discloses, "The implantable medical device also includes a wireless transmitter/receiver unit capable of establishing a communications link with a host computer (external controller)..." (Abstract, lines 9-12). Mazar goes on to disclose, "The various communications between the components of the advanced patient management system 200 (which includes the IMD) may be made securely using several different techniques. For

example, encryption and/or tunneling techniques may be used to protect data transmissions" (Paragraph 64, lines 1-5). Mazar further discloses an IMD memory in paragraph 101, lines 11-15. Mazar states, "The processor 514 comprises a microprocessor-based computer, which may include one or more processing units and a memory 516 suitable for use in an implantable medical device". From figure 5, it can be seen that there is 2-way communication between the RF receiver and the baseband processor. There is also 2-way communication between the baseband processor and the command processor. Furthermore there is 2-way communication between the command processor and the memory. Therefore, the memory is considered to be coupled to the receiver. Mazar further discloses, "Encryption, authentication, and verification techniques may also be used to detect and correct data transmission errors" (Paragraph 64, lines 16-18). However, Mazar fails to teach that the encryption method includes the generation and implementation of a key and hash values. Abdulkader, on the other hand, discloses an encryption method which requires the implementation of a key and hash values. Abdulkader discloses, "In order to secure the original data against modification by an intruder, it is a common practice to apply a one-way cryptographic hash function on the original text of the message. In this approach, a one-way hash function is applied on the original content. This function results in value that is usually fixed in length. The resultant value is then encrypted using an encryption key (here, the key is generated and stored). The receiver of the message performs the same

operation and compares the results of the one-way cryptographic hash function (Therefore, a hash generator and a comparator must be present). If the results are the same, the receiver can conclude that the received message is authentic. In this invention, the use of one-way hash function implies the generation of the hash value that is followed by an encryption step" (Paragraph 6). Therefore, it would have been obvious to one of ordinary skill in the art to modify the device of Mazar in view of the teachings of Abdulkader, to incorporate a previously disclosed encryption method.

4. In regard to claim 6, see FIG. 5 of Mazar et al. (US 2004/0122489). From this figure, it can be seen that there is a 2-way connection between the Therapy and Sense Module and the Command and Control Processor. Furthermore, the Command and Control Processor is connected to the Baseband Processor by means of a 2-way connection, which is connected to the receiver by means of a 2-way connection. Therefore, the "therapy or monitoring circuit" is coupled to the receiver.

5. In regard to claim 7, Mazar discloses, "Some devices, such as legacy implanted cardiac rhythm management ("CRM") devices, communicate via an internal transceiver that communicates with an external programmer. The communication range of such devices is typically 4-12 inches" (Paragraph 51, lines 1-5). It is well known in the art to use inductive telemetry to control implanted devices such as CRM devices and that the range of this telemetry is fairly small (4-12 inches).

Therefore, the examiner considers this transceiver to be performing inductive telemetry.

6. In regard to claim 8, it would be obvious to one of ordinary skill in the art to implement an SHA-1 algorithm in the hash value generator, since SHA-1 algorithms are the most commonly used security hash algorithms.

7. In regard to claim 13, see rejections for claim 1 and 7. Here, the inductive telemetry is considered by the examiner to be the near field communication link.

8. In regard to claim 47, see rejection for claim 1. For purposes of this claim, the implantable device is considered by the examiner to be the "first device" and the computer (external controller) is considered by the examiner to be the "second device".

9. In regard to claim 9, a hash value generator would inherently have executable directions in order to generate the hash values necessary to encode the message.

10. In regard to claim 11, see the rejection for claims 1 and 10. Here, the examiner takes the "code" to be the first hash value that is generated, which in turn leads to the generation of the second hash value.

11. In regard to claim 14, Mazar discloses, "The implantable medical device also includes a wireless transmitter/receiver unit capable of establishing a communications link with a host computer (external controller)..." (Abstract, lines 9-12). Mazar goes on to disclose, "The various communications between the components of the advanced patient management system 200 (which includes

the IMD) may be made securely using several different techniques. For example, encryption and/or tunneling techniques may be used to protect data transmissions" (Paragraph 64, lines 1-5). Since the host computer communicates with the IMD and because the IMD has a transmitter, the computer must therefore have a receiver, which is configured to receive data from the IMD. Mazar further discloses, "Encryption, authentication, and verification techniques may also be used to detect and correct data transmission errors" (Paragraph 64, lines 16-18). However, Mazar fails to teach that the encryption method includes the generation and implementation of a key and hash values. Abdulkader, on the other hand, discloses an encryption method, which requires the implementation of a key and hash values. Abdulkader discloses, "In order to secure the original data against modification by an intruder, it is a common practice to apply a one-way cryptographic hash function on the original text of the message. In this approach, a one-way hash function is applied on the original content. This function results in value that is usually fixed in length. The resultant value is then encrypted using an encryption key. The receiver of the message performs the same operation and compares the results of the one-way cryptographic hash function (Therefore, a hash generator and a comparator must be present). If the results are the same, the receiver can conclude that the received message is authentic. In this invention, the use of one-way hash function implies the generation of the hash value that is followed by an encryption step" (Paragraph 6). Therefore, it would have been obvious to

one of ordinary skill in the art to modify the device of Mazar in view of the teachings of Abdulkader, to incorporate a previously disclosed encryption method.

12. In regard to claim 15, Mazar discloses, "Some devices, such as legacy implanted cardiac rhythm management ("CRM") devices, communicate via an internal transceiver that communicates with an external programmer. The communication range of such devices is typically 4-12 inches" (Paragraph 51, lines 1-5). This is considered by the examiner to be a form of near-field telemetry

13. In regard to claim 16, Mazar discloses, "The implantable medical device also includes a wireless transmitter/receiver unit capable of establishing a communications link with a host computer over the long-range wireless network" (Abstract, lines 9-12). This is considered by the examiner to be far field telemetry.

14. In regard to claim 25, see rejections for claims 1 and 14. Here, the external device is a computer with a far field transceiver. Since a computer is known to have a memory and a processor, which are coupled together on a motherboard, the "external device" contains a processor coupled to a memory. Furthermore, all computers are known to have data ports, which are used to send data back and forth from the external source and the memory and the processor of the computer. From the rejections for claims 1 and 14, it can be seen that the external processor (computer) is adapted to execute instructions to generate a first hash value, a key, and a message and is capable of sending this message

and hash value to the implanted device where it can be decoded by the IMD and checked for authenticity through the implementation of a comparator.

15. In regard to claims 26 and 27, see rejections for claims 7 and 25. It is well known in the art to use coils to perform inductive telemetry. Furthermore, in order to perform inductive telemetry between two devices, a telemetry coil would be required in both devices to allow for the data transmission to occur.

16. In regard to claims 28 and 29, see Figure 5 of the Mazar reference. Here, Elements 522A and 522B of the IMD are connected to a "Therapy and Sensor Module" which is considered by the examiner to be both a therapy circuit and a monitor circuit. The sensor portion of the circuit "monitors" heart activity.

17. In regard to claim 30, Mazar discloses, "The implantable medical device also includes a wireless transmitter/receiver unit capable of establishing a communications link with a host computer (external controller)..." (Abstract, lines 9-12). A computer is known to have data ports for a keyboard, a mouse, a data storage device (flash drive, external hard drive, zip drives, etc.), a network connection (dial up, cable modem, DSL, LAN, modem, etc.), and a data bus.

18. In regard to claims 53, see rejections for claims 7 and 47. Here, the key is being transmitted from the external device to the implanted device through inductive telemetry, which the examiner considers to be "inductive coupling".

19. In regard to claim 56, a hash value generator is used. The hash value generator is controlled by a "hash function" to vary the hash value being generated. The examiner considers this "hash function" to be a "hashing algorithm".

20. Claims 3, 4, 12, 17, 18, 48, and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mazar et al. (US 2004/0122489) in view of Abdulkader (US 2002/0120838) in further view of Silverbrook (US 2004/0168071).

21. In regard to claims 3 and 4, Mazar in view of Abdulkader, as discussed above, discloses an implantable medical device that is capable of receiving an encrypted message, generating a corresponding hash value in response to the message, and authenticating the message by comparing the hash values. However, Mazar in view of Abdulkader fails to teach that the device has its own number generator. Silverbrook, on the other hand, teaches that a hash value generator is a random number generator and that the device therefore does have a random number generator, which provides the second hash value. Silverbrook discloses, "The actual type of random number generator required will depend upon the implementation and the purposes for which the generator is used. Generators include Blum...hash functions, such as SHA-1 and RIPEMD-160, and..." (Paragraph 154, lines 32-37). Therefore, the device of Mazar in view of Abdulkader does contain a random number generator.

22. In regard to claims 2 and 12, Mazar et al. (US 2004/0122489) in view of Abdulkader (US 2002/0120838), as discussed above, discloses a method for an implantable device to receive an encrypted message, generate a second hash value from this message and authenticate the message by comparing the hash

values. However, Mazar in view of Abdulkader fails to teach that the second hash value is generated as a function of a number provided by the number generator. Silverbrook, on the other hand, teaches that it is common in the art for a "code" (in this case, a hash value) to include a time stamp. Silverbrook discloses, "Consequently, messages often include a random number and a time stamp to ensure that the message (and hence its encrypted counterpart) varies each time. Random number generators are also often used to generate keys" (Paragraph 154, lines 16-19). Therefore, it would have been obvious for one of ordinary skill in the art to include a time stamp along with the "code" that was being sent, since it is common to do so in the art. It would have also been obvious to one of ordinary skill in the art to include a device, such as a clock, in the implantable device in order to provide the necessary time stamp

23. In regard to claims 17 and 18, Mazar in view of Abdulkader, as discussed above, teaches a nonimplantable device that is configured to receive data from an implantable device, generate a second hash value as a function of the message, and authenticate the message by comparing the two hash values. However, Mazar in view of Abdulkader fails to teach a "freshness code" for a subsequent message. Silverbrook, on the other hand, teaches, "Consequently, messages often include a random number and a time stamp to ensure that the message (and hence its encrypted counterpart) varies each time. Random number generators are also often used to generate keys" (Paragraph 154, lines 16-19). Silverbrook further teaches, "The actual type of random number generator

required will depend upon the implementation and the purposes for which the generator is used. Generators include Blum...hash functions, such as SHA-1 and RIPEMD-160, and..." (Paragraph 154, lines 32-37). The "code generator" is the hash value function, which is a random number generator that creates the hash values. Therefore, it would have been obvious to one of ordinary skill in the art to modify the device of Mazar in view of Abdulkader in further view of the teachings of Silverbrook to create a nonimplantable device with a "freshness code" to prevent the messages that it sends/receives to/from the implantable device from being seen or modified by a third party, which could in turn lead to an attack.

24. In regard to claims 48, and 49, Mazar in view of Abdulkader teaches an implantable device working in conjunction with an external controller, wherein the external controller sends an encrypted message to the implantable device, where it is decrypted, another hash value is generated, and the message is authenticated through hash value comparison. However, Mazar in view of Abdulkader fails to teach that the code that is received by the implantable device is a random number. Silverbrook, on the other hand, teaches, "Consequently, messages often include a random number and a time stamp to ensure that the message (and hence its encrypted counterpart) varies each time. Random number generators are also often used to generate keys" (Paragraph 154, lines 16-19). Silverbrook further teaches, "The actual type of random number generator required will depend upon the implementation and the purposes for

which the generator is used. Generators include Blum...hash functions, such as SHA-1 and RIPEMD-160, and..." (Paragraph 154, lines 32-37). Since the hash value generator is a random number generator, a random number is sent. Furthermore, it would have been obvious to one of ordinary skill in the art to modify the device of Mazar in view of Abdulkader in further view of the teachings of Silverbrook since using a random number and a time stamp to encrypt a message is a common technique used in the art.

25. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mazar et al. (US 2004/0122489) in view of Abdulkader (US 2002/0120838) in further view of the teachings of Madoukh (US 2001/0019614). Mazar in view of Abdulkader, as discussed above, discloses an implantable device with a receiver capable of receiving an encrypted message with a hash function, creating its own hash function in response to the original message and the key, and authenticating the message by comparing the two hash values. However, Mazar in view of Abdulkader fails to teach that the key is generated dynamically. Madoukh, on the other hand, teaches an encryption method which implements the use of a dynamic key generator. Madoukh discloses, "In 9one embodiment, the encryption keys are preferably dynamic and rotate with high frequency...The encryption keys are dynamic inn that when an encryption key expires, the computer system will retrieve all data encrypted with the old encryption key and use a new encryption key to encrypt the data" (Paragraph 7, lines 4-13). It would

have been obvious to one of ordinary skill in the art to modify the device of Mazar in view of Abdulkader in further view of the teachings of Madoukh in order to create a device with an encryption method that was harder to decode.

26. Claim 57-59 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mazar et al. (US 2004/0122489) in view of Abdulkader (US 2002/0120838) in further view of the teachings of Zotto et al. (US 2004/0009815).

27. In regard to claims 57-59, Mazar in view of Abdulkader, as discussed above, discloses an implantable device with a receiver capable of receiving an encrypted message with a hash function, creating its own hash function in response to the original message and the key, and authenticating the message by comparing the two hash values. However, Mazar in view of Abdulkader fails to teach that the encryption includes a hash standard algorithm along with a message digest algorithm. Zotto, on the other hand, teaches the use of both a SHA and a message digest in order to encrypt a message. Zotto discloses, "In one implementation, this verification inn act 164 is performed using public/private key encryption and a digest. Content source 106 stores, for each piece of content that it stores, a digest of that content. The digest of a piece of content can be generated in any of a variety of conventional manners, such as by using a conventional hashing algorithm (e.g., Message Digest 2 (MD2)...Secure Hash Algorithm (SHA), SHA-1, etc.)...content source 106 also has a public/private key pair associated with it, and uses its private key to encrypt each such digest"

(Paragraph 35). It would have been obvious for one of obvious skill in the art to modify the device of Mazar in view of Abdulkader in further view of the teachings of Zotto in order to create a device that is more secure.

Allowable Subject Matter

28. Claim 50, 51, 54, and 55 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joy P. Patel whose telephone number is 571-272-5556. The examiner can normally be reached on Monday-Friday 8:30-5:00. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Robert Pezzuto can be reached on (571)-272-6996. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Robert E. Pezzuto
Supervisory patent Examiner
Art Unit 3766

Joy Patel
Patent Examiner
Art Unit 3766